Volume 14, Issue 16   Atari Online News, Etc.   April 20, 2012

=~=~=~=

A-ONE #1416   04/20/12

~ Pentagon Sees Progress ~ People Are Talking!   ~ The My Tablet 7!
~ Courtroom Tweets Battle ~ ICANN Glitch Festers! ~ FCC Fines Google!
~ "Different" Win 8 Users ~ 20% Adults, No Web Use ~ Smaller iPad Rumors!

```
       ~ You May Lose Internet!  ~ US Slams the Aussies!  ~ New Mexico Must Pay!

                        -* UK's War on Internet Freedom *-
                        -* Week of Action Against CISPA Begins *-
                      -* China Internet Censorship Futile: Ai Weiwei *-




                                    =~=~=~=



->From the Editor's Keyboard                    "Saying it like it is!"
  """"""""""""""""""""""""""""



The work continues to try and get things a bit more stabilized with our
family matters.  Nothing is simple any more - red tape mixed with even more
red tape!  One step forward, three steps backward, it seems.  But, we're
trying to stay on top of things here as best as possible.

I wish that I had more time and mindset to talk about various current
affairs, but my mind is elsewhere; and "free" time just isn't there.  So,
typically, it seems lately, I'll just move on to this week's issue.

Until next time...




                                    =~=~=~=



                            A-ONE's Headline News
                       The Latest in Computer Technology News
                           Compiled by: Dana P. Jacobson



                 Pentagon Sees Progress, Challenges in Cyber Warfare


The Pentagon says it is making progress in developing weapons for its
newest battleground - cyberspace - but still faces funding, technology
and policy challenges.

U.S. Air Force Lieutenant General Michael Basla, vice commander of Air
Force Space Command, told industry officials on Monday the service was
approaching its work on cyber capability as it would any other major
weapons system.

"We have made measurable progress in defensive and offensive capabilities"
in the past year, Basla said at a space conference.

He talked about teams of cyber "hunters" and listed several new programs -
all part of the Pentagon's new drive to be more transparent about its work
on cyber warfare and push back against daily attacks on its computer
systems.
```

A watershed U.S. intelligence report in November said China and Russia are using cyber espionage to steal U.S. trade and technology secrets. Last week, the head of intelligence at U.S. Cyber Command described what he called an accelerating "global cyber arms race."

Basla said Washington was keeping a close eye on cyber skills being developed by Russia and China, and the U.S. government has made it clear that it reserved the right to protect itself from cyber attacks, just like other attacks.

He said those countries had clearly penetrated U.S. networks.

Basla said escalating threats meant the cyber area was one of few that might see a slight increase in funding in coming years even as projected U.S. military spending is due to decline by $487 billion over the next 10 years.

But he said military leaders would have trouble meeting all their cyber mission priorities if U.S. lawmakers don't avert an extra $500 billion in defense spending cuts, or sequestration.

"The Air Force or the department may have to make some hard choices about giving up resources in other areas," if spending is cut further, Basla told reporters. The Air Force's primary mission - to safeguard the country's nuclear weapons - would be protected from the cuts, he said.

Basla said U.S. computer networks were under constant attack, and the military's dependence on those networks for every aspect of war fighting was recognized by the country's adversaries, who saw it as the country's "soft underbelly."

"This is a journey versus a short sprint here," he said. "This is a marathon that we'll continue to work."

He described technical stumbling blocks in Air Force efforts to create a single, more defensible computer work environment - it had to replace brand-new computer servers to handle it - and said service members needed to take precautions using the Internet, even away from work.

The Defense Department announced a new cyber strategy last year and each of the armed services has a cyber division.

Madelyn Creedon, assistant secretary of defense for global strategic affairs, told the Space Foundation conference the United States viewed efforts by other countries to sneak into its computer networks and steal U.S. weapons development plans "one of the most serious long term threats" it faces.

   Week of Action Against CISPA Begins, But Don't Expect Web Blackouts

Internet advocacy groups have launched a "Week of Action" to raise awareness of the Cyber Intelligence Sharing and Protection Act (CISPA) and other cybersecurity bills which they believe pose a dire threat to the privacy and security of web users.

The organizations leading the protests include many of the same groups that fiercely opposed the Stop Online Piracy Act (SOPA), such as the

Electronic Frontier Foundation, the Center for Democracy and Technology and the American Civil Liberties Union.

The week of action will feature an informational campaign aiming to teach people about cybersecurity bills currently in Congress as well as the promotion of tools which citizens can use to contact lawmakers about those bills. There are no SOPA-style blackouts of any major sites being planned. Instead, the groups involved are sticking to social media outreach, petitions and other techniques that proved effective when the battle over SOPA came to a head.

CISPA, introduced by Rep. Mike Rogers (R-Mich.), is intended to allow private businesses and the government to share information about potential cybersecurity threats to prevent theft of intellectual property and bolster national security.

However, groups such as ACLU believe that CISPA's language is dangerously broad and would allow the government to spy on private emails, text messages and social media messages.

"H.R. 3523, the Cybersecurity Information Sharing and Protection Act (CISPA), promoted as a measure to counter cyber attacks, would allow the NSA to collect the internet records of people who are not suspected of doing anything wrong," says a petition hosted by the ACLU.

The EFF also considers CISPA to be a threat to privacy.

"We want Congress to reject legislation that uses dangerously vague language to define the breadth of data that can be shared with the government, hands the reins of America s cybersecurity defenses to the NSA – an agency with no transparency and little accountability – and allows data shared with the government to be used for purposes unrelated to cybersecurity," says Rebecca Jeschke, media relations director at the EFF.

When major websites such as Wikipedia and Reddit shut their digital doors and Google hosted an anti-SOPA petition on Jan. 18, they generated tens of thousands of calls, tweets and emails to lawmakers. However, Brock Meeks of the Center for Democracy and Technology says that the planners are currently focused on spreading information about the bill without blacking out websites that could be used to foster conversation about cybersecurity and privacy.

"We're doing it to raise awareness of the serious civil liberties and privacy concerns that are still present in CISPA," says Meeks.

Meeks added that the planners are aware that CISPA is a draft under discussion – the goal, he says, is to get their concerns about the bill into that conversation by raising awareness and encouraging people to make calls to Congress.

"We know that there is a lot of discussion, people up on the Hill are open to exploring additional changes in their bill and that's certainly welcome," says Meeks. "The aim of this week is to raise awareness and have people call members of Congress to tell them that they want certain provisions taken out of the bill and have the language narrowed to make sure it's used only for cybersecurity."

The House Intelligence Committee released an updated discussion draft of CISPA on Friday. Susan Phalen, communications director of that committee,

says that posting was part of a continuing effort to increase transparency around the bill. The committee recently opened a Twitter account, @HouseIntelComm, which has been tweeting almost exclusively about CISPA.

China Internet Censorship Futile: Ai Weiwei

Dissident artist Ai Weiwei warned the Chinese government that its attempts to censor the internet would inevitably fail, in an article published in Monday's Guardian newspaper.

Ai, who was held for 81 days last year as police rounded up dissidents amid online calls for Arab-style protests in China, wrote in the British newspaper that new "real identity" rules to curb troublesome microbloggers would only "push the problem to the next generation".

"In the long run, they (the government) must understand it's not possible for them to control the internet unless they shut it off - and they can't live with the consequences of that," he wrote.

"The people will always have the last word - even if someone has a very weak, quiet voice. Such power will collapse because of a whisper.

"The internet is uncontrollable. And if the internet is uncontrollable, freedom will win. It's as simple as that," he added.

Separately, Google co-founder Sergey Brin told the paper that online freedom was under severe threat from governments and giant internet firms like Facebook.

"I am more worried than I have been in the past," he said. "It's scary."

He cited "powerful forces", including countries eager to control the communication channels of their citizens, the entertainment industry's keenness to stamp out piracy and the software constraints imposed by firms such as Facebook and Apple.

The 38-year-old billionaire, who was reported to be behind Google's partial withdrawal from China in 2010, disagreed with Ai's belief that China would have to loosen its censorship laws.

"I thought there was no way to put the genie back in the bottle, but now it seems in certain areas the genie has been put back in the bottle," he told the Guardian.

Brin also claimed that Google would not have survived in today's climate due to the control that Facebook, which is due for a mammoth stock market flotation, exerts over the internet.

FCC Fines Google $25,000 for Unauthorized Data Collection and Impeding Investigation

The Federal Communications Commission has fined Google $25,000 for impeding a U.S. investigation into the data collection scandal surrounding its

Street View project, in which the Internet giant allegedly accessed unsecured networks and collected personal information without users permission. The FCC said the Mountain View-based company did not cooperate with the investigation and refused to reveal the names of its engineers associated with the project. "Google refused to identify any employees or produce any e-mails. The company could not supply compliant declarations without identifying employees it preferred not to identify," the FCC said. "Misconduct of this nature threatens to compromise the commission s ability to effectively investigate possible violations of the Communications Act and the commission s rules."

In a statement provided to Reuters, Google challenged the agency s findings and claimed it turned over the proper information. "As the FCC notes in their report, we provided all the materials the regulators felt they needed to conclude their investigation and we were not found to have violated any laws," the company said. "We disagree with the FCC s characterization of our cooperation in their investigation and will be filing a response."

The UK Government's War on Internet Freedom

Last summer in the wake of the London riots, British Prime Minister David Cameron insisted that the government should have the power to censor social media and "stop [alleged rioters] from communicating via these websites". But after Cameron's plan was widely compared to the tactics of former Egypt President Hosni Mubarak – not to mention the same social media services were instrumental in helping organise post-riot cleanup – the proposal never materialised.

Unfortunately, Cameron's declaration that the "free flow of information" can sometimes be a problem, then an aberration, seems to have turned into a pillar of the UK government's 2012 agenda. Despite declaring early on in his term that internet freedom should be respected "in Tahrir Square as much as Trafalgar Square", his government is now considering a series of laws that would dramatically restrict online privacy and freedom of speech.

The most controversial plan, strongly defended by Cameron last week, would allow the government to monitor every email, text message and phone call flowing throughout the country. Internet service providers (ISPs) would be forced to install hardware that would give law enforcement real time, on-demand access to every internet user's IP address, email address books, when and to whom emails are sent and how frequently – as well as the same type of data for phone calls and text messages.

Because many popular services – like Google and Facebook – encrypt the transmission of user data, the government also would force social media sites and other online service providers to comply with any data request. Currently, according to their most recent Transparency Report, Google refused to comply with 37 per cent of user data requests they received from UK authorities in the first six months of 2011, because they didn't comport with "the spirit or letter of the law", likely indicating overly broad requests or that the authorities provided no reasonable suspicion of a crime occurred. Under the new proposal, Google could not refuse any requests – regardless of their validity – and would be forced to hand over all data.

Cameron said his proposal was meant "to keep our country safe from serious and organised crime and also from terrorist threats that - that we still face in this country". But as Privacy International explained: "In a terrorism investigation, the police will already have access to all the data they could want. This is about other investigations." The information gathered in this new programme would be available to local law enforcement for use in any investigation and would be available without any judicial oversight.

Parliament has also targeted Google and Facebook on the censorship front in recent weeks. As the Guardian reported, "A cross-party committee of MPs and peers has urged the government to consider introducing legislation that would force Google to censor its search results to block material that a court has found to be in breach of someone's privacy." By "privacy", the committee meant so-called "super-injunctions" - censorship orders, usually taken out by celebrities or wealthy individuals, which ban a publisher from mentioning a topic or even the injunction.

In the last year, users on Twitter and Google have broken several super-injunctions. For example, a Scottish oil company obtained a super-injunction against Greenpeace to keep photographs of the environmental group's protest off social media sites. Within hours, unaffiliated users posted hundreds of the pictures, effectively nullifying the order. If the recommendation by the MPs were followed, Google, Facebook and Twitter would have to proactively monitor and remove such results from their webpages.

Another bill, known as the Online Safety Act, would force ISPs and mobile network providers to automatically block porn by default. As the Daily Tech reported, "In order to gain access to pornographic material, a user that is over 18 years of age must call their provider and ask for it directly." And if the site doesn't build in its own age verification policy, users over 18 could still be denied access even if they've opted in.

The Prime Minister is also reportedly considering rules requiring websites playing music videos to install age verification systems, because some music videos produced by popular artists like Rihanna, BeyoncØ and Madonna are allegedly "highly suggestive".

And if the government gets its way with its new copyright proposal, the only music video sites users would able to access at all would be those sanctioned by record-companies. Despite the enormous backlash over the Stop Online Piracy Act (SOPA) in the US, the UK government is reportedly trying to broker a backroom deal between ISPs and content companies in which search engines would start "voluntarily" censoring sites accused of copyright infringement. The deal would force search engines to blacklist entire websites from search results merely upon an allegation of infringement, and artificially promote "approved" websites.

Unfortunately, laws already on the books in the UK are notorious for restricting free speech as well. Their strict libel laws attract "libel tourism", where citizens from other countries go to sue for libel with cases they could never sue for in their home country. Just recently, one man was forced to pay 90,000 pounds (plus costs) because of two tweets that were seen by an estimated 65 people in England and Wales.

Libel cases in the UK cost an average of 140 times of those in the rest of Europe, according to a Cambridge University study, so people often

settle out of fear of extraordinary cost of defence, even if innocent. The UN Committee on Human Rights warned that the current system "served to discourage critical media reporting on matters of serious public interest, adversely affecting the ability of scholars and journalists to publish their work". Thankfully, the government has indicated they wish to reform the law and The Hindu reported that a Defamation Bill may be announced this year.

A UK judge recently sentenced a 21-year-old college student to 56 days in jail for a series of "racially offensive comments" written in series of tweets referring to a popular football player. The judge in the case noted, the comments were "vile and abhorrent", but "In my view, there is no alternative to an immediate prison sentence." The case, which made national and international headlines surely gave the racist remarks a far higher audience than if they had been ignored.

Beyond the domestic free speech issues, Britain is home to many of the companies exporting high tech surveillance equipment to authoritarian countries in the Middle East, where it is used to track journalists and democratic activists. The technology, which can be used to monitor a country's emails and phone calls, is similar to what the UK government will have to install to implement its own mass surveillance programme.

The British government claims it is "actively looking at this issue" and "working within the EU to introduce new controls on surveillance", but given its domestic censorship and surveillance proposals, maybe they should also exert some control at home as well.

US Slams Australia s On-Shore Cloud Fixation

The Office of the United States Trade Representative (USTR), recently released "The 2012 National Trade Estimate Report on Foreign Trade Barriers (NTE)," that surveys significant foreign barriers to US exports. The issue of cloud computing was a major barrier, it was felt.

A number of US companies had expressed concerns that various departments in the Australian Government, namely, the Department of Defence, The National Archives of Australia, the Department of Finance and Deregulation, the Australian Government Information Management Office (AGIMO) and the State of Victoria s Privacy Commissioner had been sending negative messages about cloud providers based outside the country, implying that "hosting data overseas, including in the United States, by definition entails greater risk and unduly exposes consumers to their data being scrutinised by foreign governments."

The cloud issue is not a new one. In August 2011, the global head of CSC s cloud business, Siki Giunta who was present in Australia to launch BizCloud commented that she felt that there was a lack of collaboration between the Information and Communication Technologies (ICT) industry and the Government in Australia. However, Glenn Archer, First Assistant Secretary at AGIMO, said the AGIMO had, in fact, been working very closely with industry for many months through the Australian Information Industry Association (AIIA) Cloud Task Force.

Recently, Acting Victorian Privacy Commissioner Anthony Bendall highlighted some of the privacy concerns with cloud computing, particularly in its use by the local government. He said the main

problems were the lack of control over stored data and privacy, in overseas cloud service providers. He felt that data security; accountability for data breach; and differing privacy laws were concerns that needed to be addressed, when considering storing information and data, especially relating to the government, in a cloud.

On the issue of privacy concerns, the report stated that there seemed to be a misinterpretation of the applicable US law including the US Patriot Act and regulatory requirements. In November last year, draft legislation had been introduced in Parliament, banning the overseas storing of Australian electronic health records. The report claimed this to be a significant trade barrier for US information technology companies with data centres in the US and other countries. US industry sources have appealed asking for a risk-based approach to ensure the security of sensitive data as against a geographical one.

In the telecom section, the report stated that the structure of the National Broadband Network Company, NBN Co, (responsible for implementing wholesale broadband services in Australia) could enhance non-discriminatory access to network services for overseas companies including US companies, as the NBN would not compete in retail markets. The United States expressed concern that foreign equity limits in Telstra, were still capped at 35 percent, and the individual foreign investors could own only up to 5 per cent of the company. The report stated that the US Government would monitor the development of the NBN to ensure that competitors obtained fair access to services and customers.

Judges, Journalists Clash Over Courtroom Tweets

Getting news from a big trial once took days, moving at the speed of a carrier pigeon or an express pony. The telegraph and telephone cut that time dramatically, as did live television broadcasts.

Now comes Twitter with more changes, breaking up courtroom journalism into bite-size reports that take shape as fast as a reporter can tap 140 characters into a smartphone. But the micro-blogging site is increasingly putting reporters on a collision course with judges who fear it could threaten a defendant's right to a fair trial.

The tension was highlighted recently by a Chicago court's decision to ban anyone from tweeting or using other social media at the upcoming trial of a man accused of killing Oscar winner Jennifer Hudson's family. Reporters and their advocates insist the practice is essential to providing a play-by-play for the public as justice unfolds.

"We're troubled by this ban," said Ed Yohnka, Chicago spokesman for the American Civil Liberties Union. Tweeting and social media are "merely the 21st century version of what reporters have always done - gather information and disseminate it."

Judges, he said, should embrace Twitter as a way to shed light on the judicial process, which, for many Americans, remains shrouded in mysterious ritual.

The judge in the Illinois case fears that feverish tweeting on smartphones could distract jurors and witnesses when testimony begins April 23.

"Tweeting takes away from the dignity of a courtroom," said Irv Miller, media liaison for Cook County Judge Charles Burns. "The judge doesn't want the trial to turn into a circus."

Burns is allowing reporters to bring cellphones and to send e-mails periodically, a notable concession in a state that has only recently announced it will begin experimenting with cameras in court and where cellphones are often barred from courtrooms altogether.

There's also an overflow courtroom where reporters can tweet freely. But there will be no audio or video of proceedings in the room, just live transcripts scrolling across a screen.

The issue extends beyond journalists to jurors, whose tweets have raised issues of their own across the country.

Last year, the Arkansas Supreme Court threw out a death row inmate's murder conviction after one juror tweeted during proceedings and another slept. Juror Randy Franco's tweets ranged from the philosophical to the mundane. One read, "The coffee sucks here." Less than an hour before the jury returned with a verdict, he tweeted, "It's all over."

There's little gray area regarding jurors tweeting. The Arkansas trial judge had warned jurors, "Don't Twitter anybody" about the case. Burns was similarly explicit during jury selection in Chicago.

But there's no consensus among either state or federal judges about the propriety of in-court tweets, so individual judges are often left to craft their own rules.

For instance, the judge in the child sexual abuse case of former Penn State assistant football coach Jerry Sandusky has allowed reporters to tweet from pretrial hearings but not to transmit verbatim accounts or to take photographs. Judge John Cleland hasn't indicated whether he will change that policy for the June trial.

In some ways, Judge Burns has gone further than others.

To ensure his ban is respected, he's assigned a member of the sheriff's department to track reporters' Twitter accounts while court is in session. To get accreditation to cover the trial, reporters had to disclose their Twitter handles.

If there appears to be a tweet from inside the courtroom, Penny Mateck will report it to the judge. "He'll decide what action to take," she said. Penalties could include contempt-of-court sanctions.

Peter Scheer, director of the California-based First Amendment Coalition, said having a sheriff's employee monitor tweets makes him uneasy, but it doesn't seem to violate anyone's rights because most Twitter feeds are already open for anyone to see.

Still, some observers are puzzled why e-mails would be OK, but tweets are out of order.

The judge, Miller explained, believes that having reporters constantly hunched over their phones pecking out tweets is more disruptive than sending an email every 10 or 15 minutes.

"We have been dealing with this issue of tweeting in court a lot these days - but this is an approach I have never heard of before. It's weird," said Lucy Dalglish, director of the Virginia-based Reporters Committee for Freedom of the Press.

She wondered if there wasn't a greater risk of inaccuracies when reporters at the scene e-mailed colleagues at news bureaus, who then put their own interpretation on emailed text and published it on websites or their own Twitter accounts.

Radio journalist Jennifer Fuller is equally perplexed.

"We've been taking notes in courts for years," said Fuller, president of the Illinois News Broadcasters Association. "If a dozen reporters put their heads down to start writing at the same time, couldn't you say that's as disruptive as tweeting?"

It's not just Twitter's potential to distract. Other judges worry that tweets about evidence could pop up uninvited on jurors' cellphones, possibly tainting the panel.

In their request for a new trial, attorneys for Texas financier R. Allen Stanford, who was convicted of fraud last month, argued that tweeting by reporters distracted jurors and created other risks. The federal judge denied the request without explanation.

And a Kansas judge last week declared a mistrial after a Topeka Capital-Journal reporter tweeted a photo that included the grainy profile of a juror hearing a murder case. The judge had permitted camera phones in court but said no photos were to be taken of jurors.

Reporter Ann Marie Bush hadn't realized one juror was in view, Publisher Gregg Ireland said, adding that the company "regrets the error and loss of the court's time."

Journalists understand judges' concerns, Dalglish said. But the better solution is for courts to do what they have done for decades - tell jurors not to follow news on their case, including by switching off their Twitter feeds.

One obstacle to reaching a consensus is that no one can agree on just what Twitter is or does. Some judges say it's broadcasting, like TV, which is banned from courtrooms in some states. Fuller says tweets are more like notes that get shared.

Because Twitter has become the medium through which some consumers get most of their news, it's all the more urgent for judges and journalists to come to an accommodation, Fuller said.

And her association's policy on tweeting in court?

"We don't have one yet," she said. "We're working at it. Finding a middle ground will take time."

$150 Ice Cream Sandwich-Powered Tablet Takes Aim at Kindle Fire

Amazon s affordable Kindle Fire tablet shook up the industry when it

launched last year. Tablet vendors were already having serious difficulties competing against Apple s iPad, and these companies would now have to find a way to cut costs as well. While Samsung announced last week that it will soon launch lower-priced Galaxy tablets, a new off-brand device has the potential to make waves if the firm behind it can manage to successfully fight for attention in an increasingly crowded market.

The 'My Tablet 7,' a new effort from New York-based software and hardware developer Xtex, is one of the most affordable tablets available in the United States. The entry-level 7-inch slate is already available for order direct from Xtex, and it costs just $149.99 despite specs that, in some areas, compete with several devices currently available at much higher price points.

Xtex s My Tablet 7 features a 7-inch 800 x 480-pixel display, a 1.5GHz processor, 16GB of internal storage, up to 32GB of additional SD storage, 1GB of RAM, a 2-megapixel front-facing webcam, an HDMI-out port that supports 1080p video playback, a full USB port, a miniUSB port and Android 4.0.3 Ice Cream Sandwich.

The low-resolution display is the biggest down-side here, and it remains to be seen how Ice Cream Sandwich will perform with a 1.5GHz single-core chipset running the show. At $150, however, this affordable device has the potential to appeal to a number of budget-conscious consumers on the lookout for a cheap tablet.

The company s press release follows below.

 MY TABLET, 7-INCH HIGH PERFORMANCE AND AFFORDABLE ANDROID TABLET LAUNCHES

    The $150, 7-Inch My Tablet combines portability with connectivity and up to 48GB memory

    NEW YORK - April 13, 2012 - XTEX announces My Tablet, a 7-inch WiFi enabled tablet device that combines affordability with connectivity, courtesy of the powerful and stable Android Ice Cream Sandwich 4.0.3 OS - all at a manufacturer s suggested retail price of $150.

    "Everyone is walking around with a tablet device under their arms," said XTEX VP Allen Kiehl. "The 10-inch tablet s become a fashion accessory, like not so long ago when everybody wore cell phones clipped to their belt." Eventually, the smartphone was made small enough to fit in a pocket, and it s time we did the same for tablets. 10-inch tablets are too big, while 5-inch models are too small, like squinting at a smartphone screen. The My Tablet 7-inch is just right. Not only is it about the size of a paperback book and ultra-slim to slip easily into a jacket or back pocket, but also it s loaded with features for convenience and on-the-go connectivity.

    "But just in case fashion and accessorizing are important, My Tablet is available in three colors at the time of its launch: black, white, and pink."

    Lightweight and less than half an inch thick, the 7-inch My Tablet fits in a pocket but comes loaded with features, including a 1.5MHz Processor, 1GB of RAM, a 16GB internal hard drive, expandable to 48GB of storage with a 32GB MiniSD card, a brilliant 800X480 7-inch capacitive screen, and a front facing 2MP webcam.

    My Tablet features Wi-Fi as well as USB Mini, USB Ports, a TF Card

Slot (supporting up to 32GB), and HDMI 1080P output, maximizing connectivity to the internet, printers, high density TVs, or any number of external devices for easy and reliable on-the-go access to email, movies, videos, music, and photos. Surf, browse, blog, text, email, stream, download, upload or Tweet - take care of business on the fly and stay in touch with friends and family with an affordably priced tablet that fits in your pocket. Download video and musicfrom the internet or carry them separately on 32GB MiniSD cards. The choice is up to the user.

"I can attest that the My Tablet was extremely snappy and handled all the apps I threw at it," writes Stormy Beach of the influential blog, AndroidSPIN.com. "I don t think there is a tablet out there that can offer this much goods for such a small price tag."

With its full list of features, including blisteringly fast 1.5GHz processor, 1GB of RAM, and 16GB of internal storage, AndroidSPIN also declared My Tablet "quite a powerful little device for $50 less than a Kindle Fire."

Power. Portability. Affordability. My Tablet. The whole world in your pocket!

Key product Information:

7" Capacitive screen (800X480)
1.5 MHz Processor
Android 4.0 OS
1GB RAM
16GB HD (storage)
2.0MP Front Facing Webcam
USB port
Mini USB Port
HDMI 1080P output
TF card slot (support 32GB)
Headset port

Rumors Swirl of Smaller iPad, Which Jobs Detested

Apple generates more gossip than the Kardashians.

There's a constantly spinning mill of rumors about Apple products, most of which turn out to be untrue. What's unusual this week is that talk has revived of a smaller iPad model, an idea company founder Steve Jobs derided publicly a year before he died.

Apple and its suppliers aren't commenting. Rumors of a smaller iPad, or "iPad mini" have percolated ever since the first iPad was launched two years ago. This time around, they're fed by media reports from South Korea, China and Taiwan, saying Apple has ordered Samsung screens that are 7.86 inches measured on the diagonal. That would make the screen about two-thirds the size of the current iPad, which has a diagonal measurement of 9.7 inches.

"From a competitive standpoint, we believe an iPad mini with a lower price point would be the competition's worst nightmare, says Shaw Wu, an analyst at Sterne Agee. "Most (competitors) already have a tough enough time competing against the iPad 2, as well as the new iPad."

Apple has successfully fended off competitors who have tried to sell tablets in iPad's size range. But last year, Amazon.com Inc. figured out how to crack Apple's stranglehold on tablets by making a half-size, no-frills tablet. The result was the Kindle Fire, which sells for $199 - basically, the cost of production. Amazon has sold millions of them.

Apple sells the iPod Touch for $199, but its screen is about a quarter of the size of the Kindle Fire - a big disadvantage for people who want to enjoy books, movies and games. It also sells the older iPad model for $399. It has nothing in between.

Price isn't the only reason customers might prefer a smaller tablet. A 7-inch model would fit in many handbags, unlike the current iPad.

Wu says he's seen evidence of Apple experimenting with both smaller and larger tablet screens since 2009, and doesn't sense that the release of an iPad mini is "imminent."

It could be hard for Apple to make money from an iPad-quality 7-inch tablet that sells for $299. Analysts at IHS iSuppli estimate that a smaller tablet would cost around $250 to produce, a figure that doesn't include development costs, packaging or patent royalties. That suggests Apple would price it at $329 or $349.

"The first thing you always have to keep in mind is: Apple is not going to sell an unprofitable product," says Rhoda Alexander at iSuppli.

"Going to a different screen size ends up being a ton of work," says Nate Weiner, the creator of Pocket, an application that stores Web pages and other material for later reading.

"If you take, for an example, an interface built for the iPad and try to cram it into the Kindle Fire, it just doesn't fit," he says.

However, developers who have already adapted their programs to the Kindle Fire or other 7-inch tablets wouldn't face a big hurdle in adapting to a third Apple screen size, Weiner says.

Apple's late CEO made a rare appearance on an October 2010 earnings conference call to launch a tirade against the 7-inch tablet Samsung Electronics Inc. was set to launch as the first major challenger to the iPad.

"The reason we wouldn't make a 7-inch tablet isn't because we don't want to hit a price point, it's because we don't think you can make a great tablet with a 7-inch screen," Jobs said. "The 7-inch tablets are tweeners, too big to compete with a smartphone and too small to compete with an iPad."

He said the resolution of the display could be increased to make up for the smaller size, but that would be "meaningless, unless your tablet also includes sandpaper, so that the user can sand down their fingers to around one quarter of the present size."

"There are clear limits of how close you can physically place elements on a touch screen before users cannot reliably tap, flick or pinch them. This is one of the key reasons we think the 10-inch screen size is the minimum size required to create great tablet apps," he said.

Jobs failed to mention Apple's success developing apps that use taps, flicks and pinches on the iPhone, with its 3.5-inch screen.

What Kind of Windows 8 User Will You Be?

Last night Microsoft announced three cuts of its much anticipated new operating system: Windows 8, Windows 8 Pro and Windows RT. Unlike previous incarnations of its operating systems, Microsoft pared the options down to three. But, even with just a few choices, like a pair of jeans, there's a right fit for each person.

The Windows maker didn't give any indication of the OS release date, or prices - important factors for buyers -- looking at the features, we bet we can help find the right choice for your needs.

This standard version, akin to the consumer preview, will work for almost any type of Windows user. "For many consumers, Windows 8 will be the right choice," writes Brandon LeBlanc on the Microsoft Windows blog. This version will have all the features Microsoft announced at the Mobile World Conference, including the new Metro influenced interface, navigability between gadgets, an app store and all sorts of navigation options. Microsoft has the full breakdown on that blog post. It's the simplest, most basic version of the new OS, that will fit most people's needs. For those not breathlessly following the Windows 8 hype, here's a little tour of your future OS.

As the "pro" tag indicates, this is for the more serious computing folks, like "tech enthusiasts and business/technical professionals," explains LeBlanc. It has all the same jazz as Windows 8, but dressed up a bit. It's for the type of person that wants to build things on their computer. It includes, as the post explains "features for encryption, virtualization, PC management and domain connectivity," writes LeBlanc. "Windows Media Center will be available as an economical 'media pack' add-on to Windows 8 Pro. If you are an enthusiast or you want to use your PC in a business environment, you will want Windows 8 Pro," he continues. It has the type of security and IT features that one might need in a business setting.

Though the commenters are hating on the "RT" name for its vagueness, it sounds like just the right amount of obscurity for the most forward-thinking of our three cuts. Like a skinny jean, this will only fit a certain body or fashion type, as it only runs on ARM. Microsoft has a whole long post about what ARM means, but basically, it's the technology that enables tablets and smartphones. The cool part: RT comes with Microsoft office. But unlike the other two Windows 8 systems, no other desktop apps will run on it, instead focusing on Metro based apps. So, it's a bit different.

Delay in Internet Name Expansion Continues

There's still no word on when applications will continue for new Internet address suffixes to join ".com" and others in use.

Last week, a technical glitch forced the Internet Corporation for Assigned Names and Numbers, which is in charge of domain names, to abruptly shut

down a system for letting companies and organizations apply for new names.

The system was supposed to have reopened Tuesday, but ICANN said then that it needed more time to inform applicants that may have been affected by the glitch.

ICANN now says it's still testing the fix and sifting through the data to determine which applicants were affected. It gave no target date this time. ICANN says it has ruled out hacking as the cause.

Hundreds of Thousands May Lose Internet in July

For computer users, a few mouse clicks could mean the difference between staying online and losing Internet connections this summer.

Unknown to most of them, their problem began when international hackers ran an online advertising scam to take control of infected computers around the world. In a highly unusual response, the FBI set up a safety net months ago using government computers to prevent Internet disruptions for those infected users. But that system is to be shut down.

The FBI is encouraging users to visit a website run by its security partner, http://www.dcwg.org , that will inform them whether they're infected and explain how to fix the problem. After July 9, infected users won't be able to connect to the Internet.

Most victims don't even know their computers have been infected, although the malicious software probably has slowed their web surfing and disabled their antivirus software, making their machines more vulnerable to other problems.

Last November, the FBI and other authorities were preparing to take down a hacker ring that had been running an Internet ad scam on a massive network of infected computers.

"We started to realize that we might have a little bit of a problem on our hands because ... if we just pulled the plug on their criminal infrastructure and threw everybody in jail, the victims of this were going to be without Internet service," said Tom Grasso, an FBI supervisory special agent. "The average user would open up Internet Explorer and get 'page not found' and think the Internet is broken."

On the night of the arrests, the agency brought in Paul Vixie, chairman and founder of Internet Systems Consortium, to install two Internet servers to take the place of the truckload of impounded rogue servers that infected computers were using. Federal officials planned to keep their servers online until March, giving everyone opportunity to clean their computers. But it wasn't enough time. A federal judge in New York extended the deadline until July.

Now, said Grasso, "the full court press is on to get people to address this problem." And it's up to computer users to check their PCs.

This is what happened:

Hackers infected a network of probably more than 570,000 computers worldwide. They took advantage of vulnerabilities in the Microsoft Windows

operating system to install malicious software on the victim computers. This turned off antivirus updates and changed the way the computers reconcile website addresses behind the scenes on the Internet's domain name system.

The DNS system is a network of servers that translates a web address - such as www.ap.org - into the numerical addresses that computers use. Victim computers were reprogrammed to use rogue DNS servers owned by the attackers. This allowed the attackers to redirect computers to fraudulent versions of any website.

The hackers earned profits from advertisements that appeared on websites that victims were tricked into visiting. The scam netted the hackers at least $14 million, according to the FBI. It also made thousands of computers reliant on the rogue servers for their Internet browsing.

When the FBI and others arrested six Estonians last November, the agency replaced the rogue servers with Vixie's clean ones. Installing and running the two substitute servers for eight months is costing the federal government about $87,000.

The number of victims is hard to pinpoint, but the FBI believes that on the day of the arrests, at least 568,000 unique Internet addresses were using the rogue servers. Five months later, FBI estimates that the number is down to at least 360,000. The U.S. has the most, about 85,000, federal authorities said. Other countries with more than 20,000 each include Italy, India, England and Germany. Smaller numbers are online in Spain, France, Canada, China and Mexico.

Vixie said most of the victims are probably individual home users, rather than corporations that have technology staffs who routinely check the computers.

FBI officials said they organized an unusual system to avoid any appearance of government intrusion into the Internet or private computers. And while this is the first time the FBI used it, it won't be the last.

"This is the future of what we will be doing," said Eric Strom, a unit chief in the FBI's Cyber Division. "Until there is a change in legal system, both inside and outside the United States, to get up to speed with the cyber problem, we will have to go down these paths, trail-blazing if you will, on these types of investigations."

Now, he said, every time the agency gets near the end of a cyber case, "we get to the point where we say, how are we going to do this, how are we going to clean the system" without creating a bigger mess than before.

                    Court: Online Bookseller Owes New Mexico Sales Tax

A nationally known online bookseller must pay more than a half million dollars in taxes for books, music and movies bought by customers in New Mexico, the state Court of Appeals has ruled in a dispute over the state's power to tax corporate chains and Internet shopping.

The court's decision came Wednesday in a case involving an out-of-state online business, Barnes&nobles.com, LLC, which was part of the corporate family of bookseller Barnes & Noble Inc.

The online retailer was assessed gross receipts taxes in 2006 of $534,563 for sales from 1998 to 2005. The company protested and a state agency hearing officer agreed with the company that it wasn't required to collect and pay the tax because it had no presence in the state or what is known as a "substantial nexus" with New Mexico.

The online retailer was organized under Delaware laws and it had no employees or offices in the state. However, a separate Barnes and Noble company operates three bookstores in New Mexico, with the first of those started in Albuquerque in 1996 and the most recent in Las Cruces in 2003.

Traditionally, online retailers have been required to collect taxes on sales to customers in New Mexico if the company has a physical store, a warehouse or other facilities in the state.

The Department of Taxation and Revenue contended that activities at the in-state stores, including gift cards that could be redeemed online and a membership plan that offered online discounts, created the necessary connection to New Mexico to require the Internet retailer to collect and pay the state's tax. Books purchased online also could be returned for credit at the Barnes & Noble stores in New Mexico.

The Court of Appeals said those activities alone weren't enough to justify taxing the online sales, but it concluded the "in-state use of the Barnes & Noble's trademarks was sufficient to meet the constitutional standard" to permit the New Mexico tax.

Because the trademarks were licensed to the online retailer and the company with in-state stores, Barnes & Noble "was in effect telling customers to consider taxpayers (the online retailer) and booksellers to be one and the same," the court said.

"The goodwill developed both directly, by in-store activities promoting taxpayer's website, and indirectly, by consumers' increased awareness of Barnes & Noble due to the presence of in-state stores, helped to establish and maintain a market in New Mexico for taxpayer," the court said.

Attorneys for Barnes & Noble did not immediately return telephone and email messages on Thursday seeking comment on the court ruling and whether their client plans to appeal the decision to the state Supreme Court.

A spokesman for New Mexico's tax agency declined comment because the agency expects the case to end up before the state's highest court.

The New Mexico tax currently is being collected for online sales because Barnes & Nobles has revamped the business structure of its online and in-store operations, according to court filings by company lawyers.

One in Five U.S. Adults Still Doesn t Use The Internet

The Pew Internet & American Life Project s latest poll indicates that one in five adults in the United States still doesn t use the Internet. "Senior citizens, those who prefer to take our interviews in Spanish rather than English, adults with less than a high school education, and those living in households earning less than $30,000 per year are the least likely adults to have Internet access," Pew Internet said. Almost

half of those adults who don t use the Internet found the technology
irrelevant to them, with most having never used it before. About one in
five adults claimed they didn t know enough about technology to start
using the Internet on their own, and only 10% were interested in using
the Internet or email in the future. Overall Internet adoption rates have
leveled off, however adults already online are using the Web more often
than ever before. Pew s study also showed that 88% of American adults
have a cell phone, 57% have a laptop, 19% own an eReader, 19% have a
tablet and 63% access the Internet wirelessly with one of these devices.

=~=~=~=